TO: USPTO

ZILKA·KOTAB PC

ZILKA, KOTAB & FEECE™

100 PARK CENTER PLAZA, SUITE 300
SAN JOSE, CA 95113

TELEPHONE (408) 971-2573
FAX (408) 971-4660

FAX COVER SHEET

Date:	December 15, 2006	**Phone Number**	**Fax Number**
To:	USPTO: Board of Patent Appeals and Interferences		(571) 273-8300
From:	Kevin J. Zilka		

Docket No.: NAIIP361/00.166.01 **App. No: 09/803,527**

Total Number of Pages Being Transmitted, Including Cover Sheet: 38

Message:

Please deliver to the Board of Patent Appeals and Interferences.

Thank you,

Kevin J. Zilka

☐ *Original to follow Via Regular Mail* X *Original will Not be Sent* ☐ *Original will follow Via Overnight Courier*

IF YOU DO NOT RECEIVE ALL PAGES OR IF YOU ENCOUNTER
ANY OTHER DIFFICULTY, PLEASE PHONE April
AT (408) 971-2573 AT YOUR EARLIEST CONVENIENCE

December 15, 2006

RECEIVED
CENTRAL FAX CENTER
DEC 15 2006

Practitioner's Docket No. NAI1P361_00.166.01 ***PATENT***

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: Mark J. McArdle et al.

Application No.: 09/803,527 Group No.: 2145
Filed: 03/08/2001 Examiner: Azizul Q. Choudhury
For: AUTOMATICALLY CONFIGURING A COMPUTER FIREWALL BASED ON NETWORK CONNECTION

Mail Stop Appeal Briefs – Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

TRANSMITTAL OF APPEAL BRIEF
(PATENT APPLICATION--37 C.F.R. § 41.37)

1. Transmitted herewith, is the APPEAL BRIEF in this application, with respect to the Notice of Appeal filed on May 31, 2006 and the Notice of Panel Decision from Pre-Appeal Brief Review mailed August 15, 2006.

2. STATUS OF APPLICANT

This application is on behalf of other than a small entity.

CERTIFICATION UNDER 37 C.F.R. §§ 1.8(a) and 1.10*
*(When using Express Mail, the Express Mail label number is **mandatory**; Express Mail certification is optional.)*

I hereby certify that, on the date shown below, this correspondence is being:

MAILING

__ deposited with the United States Postal Service in an envelope addressed to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

37 C.F.R. § 1.8(a)
__with sufficient postage as first class mail.

37 C.F.R. § 1.10*
__as "Express Mail Post Office to Addressee"
Mailing Label No. _____ **(mandatory)**

TRANSMISSION

✓ facsimile transmitted to the Patent and Trademark Office, (571) 273 - 8300.

Signature

Date: 12/15/2006

April Skovmand

(type or print name of person certifying)

** Only the date of filing (' 1.6) will be the date used in a patent term adjustment calculation, although the date on any certificate of mailing or transmission under ' 1.8 continues to be taken into account in determining timeliness. See ' 1.703(f). Consider "Express Mail Post Office to Addressee" (' 1.10) or facsimile transmission (' 1.6(d)) for the reply to be accorded the earliest possible filing date for patent term adjustment calculations.* 09803527

12/18/2006 MGEBREMI 00000041 09803527
01 FC:1402 ~~500.00 DA~~
02 FC:1253 1020.00 DA

RECEIVED
CENTRAL FAX CENTER
DEC 15 2006

3. FEE FOR FILING APPEAL BRIEF

Pursuant to 37 C.F.R. § 41.20(b)(2), the fee for filing the Appeal Brief is:

other than a small entity	$500.00
Appeal Brief fee due	**$500.00**

4. EXTENSION OF TERM

The proceedings herein are for a patent application and the provisions of 37 C.F.R. § 1.136 apply.

Applicant petitions for an extension of time under 37 C.F.R. § 1.136 (fees: 37 C.F.R. § 1.17(a)(1)-(5)) for three months:

Fee:	$1,020.00

If an additional extension of time is required, please consider this a petition therefor.

5. TOTAL FEE DUE

The total fee due is:

Appeal brief fee	$500.00
Extension fee (if any)	$1,020.00
TOTAL FEE DUE	**$1,520.00**

6. FEE PAYMENT

Authorization is hereby made to charge the amount of $1,520.00 to Deposit Account No. 50-1351(Order No.NAI1P361).

A duplicate of this transmittal is attached.

7. FEE DEFICIENCY

If any additional extension and/or fee is required, and if any additional fee for claims is required, charge Deposit Account No. 50-1351(Order No.NAI1P361).

Date: 12/15/06

Signature of Practitioner
Kevin J. Zilka
Zilka-Kotab, PC
P.O. Box 721120
San Jose, CA 95172

Reg. No.: 41,429
Tel. No.: 408-971-2573
Customer No.: 28875

RECEIVED
CENTRAL FAX CENTER
DEC 15 2006

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:	
McArdle et al.	Group Art Unit: 2145
Application No. 09/803,527	Examiner: Choudhury, Azizul Q.
Filed: 03/08/2001	Date: December 15, 2006
For: AUTOMATICALLY CONFIGURING A COMPUTER FIREWALL BASED ON NETWORK CONNECTION	

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

ATTENTION: Board of Patent Appeals and Interferences

APPEAL BRIEF (37 C.F.R. § 41.37)

This brief is in furtherance of the Notice of Appeal, filed in this case on May 31, 2006, and the Notice of Panel Decision from Pre-Appeal Brief Review mailed August 15, 2006.

The fees required under § 1.17, and any required petition for extension of time for filing this brief and fees therefor, are dealt with in the accompanying TRANSMITTAL OF APPEAL BRIEF.

This brief contains these items under the following headings, and in the order set forth below (37 C.F.R. § 41.37(c)(i)):

I REAL PARTY IN INTEREST
II RELATED APPEALS AND INTERFERENCES
III STATUS OF CLAIMS
IV STATUS OF AMENDMENTS
V SUMMARY OF CLAIMED SUBJECT MATTER
VI GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

VII ARGUMENT

VIII CLAIMS APPENDIX

IX EVIDENCE APPENDIX

X RELATED PROCEEDING APPENDIX

The final page of this brief bears the practitioner's signature.

I REAL PARTY IN INTEREST (37 C.F.R. § 41.37(c)(1)(i))

The real party in interest in this appeal is McAfee, Inc.

II RELATED APPEALS AND INTERFERENCES (37 C.F.R. § 41.37(c) (1)(ii))

With respect to other prior or pending appeals, interferences, or related judicial proceedings that will directly affect, or be directly affected by, or have a bearing on the Board's decision in the pending appeal, there are no other such appeals, interferences, or related judicial proceedings.

A Related Proceedings Appendix is appended hereto.

III STATUS OF CLAIMS (37 C.F.R. § 41.37(c) (1)(iii))

A. TOTAL NUMBER OF CLAIMS IN APPLICATION

Claims in the application are: 1-2, 4, 6-17, 19, 21, 24, 26, 28-32

B. STATUS OF ALL THE CLAIMS IN APPLICATION

1. Claims withdrawn from consideration: None
2. Claims pending: 1-2, 4, 6-17, 19, 21, 24, 26, 28-32
3. Claims allowed: None
4. Claims rejected: 1-2, 4, 6-17, 19, 21, 24, 26, 28-32
5. Claims cancelled: 3, 5, 18, 20, 22, 23, 25, 27, 33-43

C. CLAIMS ON APPEAL

The claims on appeal are: 1-2, 4, 6-17, 19, 21, 24, 26, 28-32

See additional status information in the Appendix of Claims.

IV STATUS OF AMENDMENTS (37 C.F.R. § 41.37(c)(1)(iv))

As to the status of any amendment filed subsequent to final rejection, an amendment was filed after a final rejection on 03/31/2006 and such amendment was entered as noted in the Advisory action mailed 04/24/2006.

V SUMMARY OF CLAIMED SUBJECT MATTER (37 C.F.R. § 41.37(c)(1)(v))

With respect to a summary of Claim 1, as shown in Figures 1A-1B, a computerized method is provided for automatically configuring a firewall (e.g. see item 103 of Figure 1A, etc.) operating within an individual computer (e.g. see item 101 of Figure 1A, etc.). In use, a zone is determined for a network address dynamically assigned to a network adapter (e.g. see item 105 of Figure 1A, etc.) in the individual computer and a security policy (e.g. see items 109 and 117 of Figures 1A and 1B respectively, etc.) for the zone is associated with the network adapter, where the security policy specifies the firewall configuration to protect the individual computer.

The security policy is defined by a policy file which includes a policy file data structure stored as an XML (extensible markup language) document. A security policy section of the policy file data structure includes an entry for each security policy that is identified by a policy identifier field and is associated with a network protocol that is identified by a protocol identifier field. In addition, the security policy section specifies filters for at least a portion of ports and services defined by the network protocol, and each port and service associated with the security policy is identified by an element identifier field, a field containing filter settings, and a log indicator field.

At least one security policy is included for a TCP/IP network and includes a PPTP (point-to-point tunneling protocol), a RIP (routing information protocol), a DHCP (dynamic host configuration protocol), an ARP (address resolution protocol), an Ident (identification protocol), ICMP (internet control message protocol) and VPN (virtual private networking) ports, and a NetBIOS (network basic input/output system) service. Further, a default setting for a high security policy on the TCP/IP network disallows incoming network traffic through the PPTP and ICMP ports. The default setting also allows incoming network traffic through the RIP, DHCP, ARP and VPN ports, disallows access through the NetBIOS service to shared resources on the individual computer, and disallows the individual computer from using shared resources of other computers on the TCP/IP network, where incoming network traffic that attempts to access the individual computer using PPTP and NetBIOS is logged.

A zone section of the policy file data structure includes an entry for each defined address zone and includes an identifier field, an address parameters field that defines the zone, and an identifier field for the security policy assigned to the zone. A default zone is defined by addresses that are outside another zone.

The determining and associating is performed when the network address for the network adapter changes. The security policy associated with the network protocol is specific to the network protocol. Additionally, the zone is defined by a set of network addresses, which comprises at least one address outside the zone.

The network address dynamically assigned to the network adapter is determined by at least one of mapping an adapter registry identifier to an associated network address stored in an operating system registry, monitoring network traffic at the network adapter and examining a predefined limited amount of the network traffic to determine the network address, and receiving a network address from a network adapter device driver when the network adapter connects to the TCP/IP network. See, for example, page 3, line 19-page 4, line 15 et al.

With respect to a summary of Claim 11, as shown in Figures 1A-1B, a computer-readable medium having computer-executable instructions is provided to automatically configure a firewall (e.g. see item 103 of Figure 1A, etc.) operating within an individual computer (e.g. see item 101 of Figure 1A, etc.). In use, a zone is determined for a network address dynamically assigned to a network adapter (e.g. see item 105 of Figure 1A, etc.) in the individual computer, and the zone is defined based on a set of network addresses, including at least one address outside the zone. In addition, a security policy for the zone is associated with the network adapter, where the security policy specifies the firewall configuration to protect the individual computer.

The security policy (e.g. see items 109 and 117 in Figures 1A and 1B respectively, etc.) is defined by a policy file which includes a policy file data structure stored as an XML (extensible markup language) document. A security policy section of the policy file data structure includes an entry for each security policy that is identified by a policy identifier field and is associated with a network protocol that is identified by a protocol identifier field.

Further, the security policy section specifies filters for at least a portion of ports and services defined by the network protocol, and each port and service associated with the security policy is identified by an element identifier field, a field containing filter settings, and a log indicator field. At least one security policy is included for a TCP/IP network and includes a PPTP (point-to-point tunneling protocol), a RIP (routing information protocol), a DHCP (dynamic host configuration protocol), an ARP (address resolution protocol), an Ident (identification protocol), ICMP (internet control message protocol) and VPN (virtual private networking) ports, and a NetBIOS (network basic input/output system) service.

Still yet, a default setting for a high security policy on the TCP/IP network disallows incoming network traffic through the PPTP and ICMP ports. The default setting also allows incoming network traffic through the RIP, DHCP, ARP and VPN ports, disallows access through the NetBIOS service to shared resources on the individual computer, and disallows the individual computer from using shared resources of other computers on the TCP/IP network, where incoming network traffic that attempts to access the individual computer using PPTP and NetBIOS is logged.

A zone section of the policy file data structure includes an entry for each defined address zone and includes an identifier field, an address parameters field that defines the zone, and an identifier field for the security policy assigned to the zone. A default zone is defined by addresses that are outside another zone. Moreover, the determining and associating is performed when the network address for the network adapter changes. The security policy associated with the network protocol is specific to the network protocol.

The network address dynamically assigned to the network adapter is determined by at least one of mapping an adapter registry identifier to an associated network address stored in an operating system registry, monitoring network traffic at the network adapter and examining a predefined limited amount of the network traffic to determine the network address, and receiving a network address from a network adapter device driver when the network adapter connects to the TCP/IP network. See, for example, page 3, line 19-page 4, line 15 et al.

With respect to a summary of Claim 21, as shown in Figures 1A,1B and 4B, a computerized system is provided that includes a processing unit (e.g. see item 55 of Figure 4B, etc.), a memory (e.g. see item 59 of Figure 4B, etc.) coupled to the processing unit through a bus (e.g. see item 57 of Figure 4B, etc.), and a network adapter (e.g. see item 105 of Figure 1A, etc.) coupled to the processing unit through the bus and further operable for coupling to a network (e.g. see items 111 and 113 in Figures 1A and 1B, respectively, etc.).

In addition, a firewall process (e.g. see item 103 of Figure 1A, etc.) is executed from the memory by the processing unit to protect the computerized system when the network adapter is coupled to a network by causing the processing unit to filter data addressed to the network adapter according to a security policy (e.g. see items 109 and 117 of Figures 1A-1B, respectively, etc.). Further, a firewall configuration process is executed from the memory by the processing unit to cause the processing unit to determine a zone for a network address dynamically assigned to the network adapter and to associate a firewall security policy for the zone with the network adapter.

The security policy is defined by a policy file which includes a policy file data structure stored as an XML (extensible markup language) document. A security policy section of the policy file data structure includes an entry for each security policy that is identified by a policy identifier field and is associated with a network protocol that is identified by a protocol identifier field. The security policy section specifies filters for at least a portion of ports and services defined by the network protocol, and each port and service associated with the security policy is identified by an element identifier field, a field containing filter settings, and a log indicator field.

At least one security policy is included for a TCP/IP network and includes a PPTP (point-to-point tunneling protocol), a RIP (routing information protocol), a DHCP (dynamic host configuration protocol), an ARP (address resolution protocol), an Ident (identification protocol), ICMP (internet control message protocol) and VPN (virtual private networking) ports, and a NetBIOS (network basic input/output system) service.

Additionally, a default setting for a high security policy on the TCP/IP network disallows incoming network traffic through the PPTP and ICMP ports. This default setting also allows incoming network traffic through the RIP, DHCP, ARP and VPN ports, disallows access through

the NetBIOS service to shared resources on the individual computer, and disallows the individual computer from using shared resources of other computers on the TCP/IP network, where incoming network traffic that attempts to access the individual computer using PPTP and NetBIOS is logged. A zone section of the policy file data structure includes an entry for each defined address zone and includes an identifier field, an address parameters field that defines the zone, and an identifier field for the security policy assigned to the zone. A default zone is defined by addresses that are outside another zone.

Still yet, the firewall configuration process is executed by the processing unit when the network address for the network adapter changes. The security policy associated with the network protocol is specific to the network protocol. The firewall configuration process further causes the processing unit to define the zone based on a set of network addresses comprising at least one address outside the zone.

The network address dynamically assigned to the network adapter is determined by at least one of mapping an adapter registry identifier to an associated network address stored in an operating system registry, monitoring network traffic at the network adapter and examining a predefined limited amount of the network traffic to determine the network address, and receiving a network address from a network adapter device driver when the network adapter connects to the TCP/IP network. See, for example, page 3, line 19-page 4, line 15 et al.

VI GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL (37 C.F.R. § 41.37(c)(1)(vi))

Following, under each issue listed, is a concise statement setting forth the corresponding ground of rejection.

Issue # 1: The Examiner has rejected Claims 1-2, 4, 6-17, 19, 21, 24, 26, and 28-32 under 35 U.S.C. 103(a) as being unpatentable over Coss et al. (U.S. Patent No. 6,098,172) in view of Minear et al. (U.S. Patent No. 5,983,350).

VII ARGUMENT (37 C.F.R. § 41.37(c)(1)(vii))

The claims of the groups noted below do not stand or fall together. In the present section, appellant explains why the claims of each group are believed to be separately patentable.

Issue # 1:

The Examiner has rejected Claims 1-2, 4, 6-17, 19, 21, 24, 26, and 28-32 under 35 U.S.C. 103(a) as being unpatentable over Coss et al. (U.S. Patent No. 6,098,172) in view of Minear et al. (U.S. Patent No. 5,983,350).

Group #1: Claims 1-2, 4, 7-9, 11-12, 14-16, 19, 21, 24, 26, 29, and 31-32

With respect to the present grouping, the Examiner has relied on the following excerpt from the Coss reference to make a prior art showing of appellant's claimed technique "wherein the security policy section specifies filters for at least a portion of ports and services defined by the network protocol, and each port and service associated with the security policy is identified by an element identifier field, a field containing filter settings, and a log indicator field" (see this or similar, but not necessarily identical language in each of the independent claims).

> "...policy to use for a new network session. Each new session must be approved by the security policies of the source domain and the destination domain(s). For connections going to the Internet, it is likely that only a single domain check is performed. The DSE makes the domain selection based on the incoming or outgoing network interface, as well as on the source or destination network address of each packet. Inclusion, in packets, of source or destination addresses allows for multiple users to be supported by a single network interface. The incoming or outgoing network interface may be in the form of a network interface card (NIC), e.g., an Intel EtherExpress Pro 100B card available from Intel Corporation.
>
> FIGS. 5A and 5B illustrate over-all flow for packet processing by a firewall which supports multiple domains. Such processing includes determining the domains which the packet is to cross, examining the applicable rules to ascertain whether the packet may pass, and determining whether any special processing is required. In the firewall..." (Col. 6, lines 49-67)

Appellant respectfully asserts that the Coss reference simply teaches the approval of new network sessions by the security policies of source and destination domains, as well as packet processing by a firewall. However, unlike the Coss reference, appellant claims the identification of each port and service associated with the security policy "by an element identifier field, a field containing filter settings, and a log indicator field," as claimed (emphasis added). As a result, appellant's claims are distinct from the Coss reference.

In the Advisory Action mailed 04/24/2006, the Examiner argued that the "Service," "Source Host," "Destination Host," "Audit Session," and "Action" categories in the chart listed in between Cols. 3 and 4 in Coss disclose appellant's claimed technique. Appellant respectfully asserts that Coss simply discloses that "[t]he security policies can be represented by sets of access rules which are represented in tabular form." However, sets of access rules in the security policy fail to disclose a technique "wherein the security policy section specifies filters for at least a portion of ports and services defined by the network protocol, and each port and service associated with the security policy is identified by an element identifier field, a field containing filter settings, and a log indicator field," as claimed by appellant (emphasis added). Moreover, appellant respectfully asserts that the "Action" category field with the description of '[r]ule action, e.g., "pass," "drop" or "proxy",' as argued by the Examiner, simply fails to disclose "a field containing filter settings," as claimed by appellant.

Further, with respect to the present grouping, the Examiner has relied on the following excerpt from the Minear reference to make a prior art showing of appellant's claimed technique "wherein a security policy section of the policy file data structure includes an entry for each security policy that is identified by a policy identifier field and is associated with a network protocol that is identified by a protocol identifier field" (see this or similar, but not necessarily identical language in each of the independent claims).

> "8. A firewall, comprising:
>
> a first communications interface;
>
> a second communications interface;
>
> a first network protocol stack connected to the first communications interface, wherein the first network protocol stack includes an Internet Protocol (IP) layer and a transport layer;

a second network protocol stack connected to the second communications interface, wherein the second network protocol stack includes an Internet Protocol (IP) layer and a transport layer;

a security policy;

a decryption procedure, operating at the IP layer of the first network protocol stack, the decryption procedure receiving encrypted messages received by said first communications interface and outputting decrypted messages; and

an application layer proxy, connected to the transport layers of said first and second network protocol stacks, wherein the application layer proxy includes a plurality of authentication protocols, wherein each authentication protocol provides a different level of security, wherein the application layer proxy receives decrypted messages from the decryption procedure, selects an authentication protocol from the plurality of authentication protocols based on the content of the decrypted message, and executes the selected authentication protocol and wherein the application layer proxy determines based on the security policy whether the message is to be forwarded, and wherein the message is returned to the IP layer if the message is to be forwarded;

a third communications interface; and

a third network protocol stack connected to the third communications interface and to the application layer proxy, wherein the third network protocol stack includes an Internet Protocol (IP) layer and a transport layer and wherein the second and third network protocol stacks are restricted to first and second burbs, respectively." (Claim 8)

Appellant respectfully asserts that the above excerpt from the Minear reference merely teaches an application layer proxy that includes a plurality of authentication protocols. Appellant, on the other hand, claims "a security policy section of the policy file data structure [that] includes an entry for each security policy that is identified by a policy identifier field and is associated with a network protocol that is identified by a protocol identifier field," as claimed (emphasis added). Since no mention is made in the above excerpt from Minear regarding the use of any identifier fields, let alone those specifically claimed by appellant, such claims are clearly distinct.

Additionally, the Examiner has not even specifically addressed appellant's claimed techniques "wherein at least one security policy is included for a TCP/IP network and includes a PPTP (point-to-point tunneling protocol), a RIP (routing information protocol), a DHCP (dynamic host configuration protocol), an ARP (address resolution protocol), an Ident (identification protocol), ICMP (internet control message protocol) and VPN (virtual private networking) ports, and a NetBIOS (network basic input/output system) service;" "wherein a zone section of the policy file

data structure includes an entry for each defined address zone and includes an identifier field, an address parameters field that defines the zone, and an identifier field for the security policy assigned to the zone;" "wherein a default zone is defined by addresses that are outside another zone;" and "wherein the security policy associated with the network protocol is specific to the network protocol." After careful review of both the Minear and Coss references, appellant notes that the above language claimed by appellant is clearly not even suggested by the prior art of record.

In the Advisory Action mailed 04/24/2006, the Examiner argued "that no limit is placed by either art as to what types of protocols can be handled within the firewall designs" and that "claim 8 of Minear's design demonstrates how multiple protocols are applicable to the design." However, appellant respectfully asserts that each "network protocol stack [is] connected to [a] communications interface," as disclosed by Minear in claim 8, simply fails to teach a technique "wherein at least one security policy is included for a TCP/IP network and includes a PPTP (point-to-point tunneling protocol), a RIP (routing information protocol), a DHCP (dynamic host configuration protocol), an ARP (address resolution protocol), an Ident (identification protocol), ICMP (internet control message protocol) and VPN (virtual private networking) ports, and a NetBIOS (network basic input/output system) service," as claimed by appellant (emphasis added).

Furthermore, with respect to the present grouping, the Examiner has simply dismissed, under Official Notice, appellant's claimed technique "wherein the security policy is defined by a policy file which includes a policy file data structure stored as an XML (extensible markup language) document" and "wherein a default setting for a high security policy on the TCP/IP network disallows incoming network traffic through the PPTP and ICMP ports, allows incoming network traffic through the RIP, DHCP, ARP and VPN ports, disallows access through the NetBIOS service to shared resources on the individual computer, and disallows the individual computer from using shared resources of other computers on the TCP/IP network, where incoming network traffic that attempts to access the individual computer using PPTP and NetBIOS is logged."

Appellant notes upon careful inspection of the prior art that neither the Coss nor the Minear references mentions the storage of a policy file data structure, much less a policy file data structure stored as an XML document, in the manner claimed by appellant. Additionally, appellant respectfully asserts that neither the Coss nor Minear references teach any sort of "default setting for a high security policy," and especially not in the foregoing detailed context claimed by appellant. Appellant thus formally requests a specific showing of the subject matter in ALL of the claims in any future action. Note excerpt from MPEP below.

> "If the applicant traverses such an [Official Notice] assertion the examiner should cite a reference in support of his or her position." See MPEP 2144.03.

In the Advisory Action mailed 04/24/2006, the Examiner, in a blanket manner, citied Greschler et al. (U.S. Patent No. 6,938,096) to meet appellant's claimed "default setting for a high security policy." Appellant has reviewed the entire Greschler reference and respectfully asserts that Greschler fails to disclose a specific technique "wherein a default setting for a high security policy on the TCP/IP network disallows incoming network traffic through the PPTP and ICMP ports, allows incoming network traffic through the RIP, DHCP, ARP and VPN ports, disallows access through the NetBIOS service to shared resources on the individual computer, and disallows the individual computer from using shared resources of other computers on the TCP/IP network, where incoming network traffic that attempts to access the individual computer using PPTP and NetBIOS is logged," as claimed by appellant.

Moreover, appellant notes that the Examiner fails to cite specific motivation in the above references to support the case for combining the Greschler reference. The Examiner is reminded that the Federal Circuit requires that there must be some logical reason apparent from the evidence of record that would justify the combination or modification of references. *In re Regel, 188 USPQ 132 (CCPA 1975).* Thus, without specific motivation, appellant respectfully asserts that reliance on such reference is inappropriate.

In the Advisory Action mailed 04/24/2006, the Examiner, again, in a blanket manner, citied Stiles et al. (U.S. Patent No. 6,842,737), Virgin et al. (U.S. Patent No. 6,826,542), and MacPhail (U.S. Patent No. 6,593,943) to meet appellant's claim language. Appellant has carefully considered the references relied upon by the Examiner, and respectfully asserts that they merely

teach usage of XML documents. The references simply fail to disclose a technique "wherein the security policy is defined by a policy file which includes a policy file data structure stored as an XML (extensible markup language) document," as claimed by appellant (emphasis added).

In addition, appellant again notes that the Examiner fails to cite specific motivation in the above references to support the case for combining the Stiles, Virgin and MacPhail references. The Examiner is again reminded that the Federal Circuit requires that there must be some logical reason apparent from the evidence of record that would justify the combination or modification of references. *In re Regel, 188 USPQ 132 (CCPA 1975).* Thus, without specific motivation, appellant respectfully asserts that reliance on such references is inappropriate.

Additionally, with respect to the present grouping, the Examiner has relied on the following excerpt from the Coss reference, along with Claim 8 from the Minear reference (reproduced above), to make a prior art showing of appellant's claimed technique "wherein the zone is defined by a set of network addresses, which comprises at least one address outside the zone" (see the same or similar, but not necessarily identical language in at least some of the aforementioned independent).

> "701: the domain table is searched for a match of the interface name;
>
> 702: if a matching table entry is found, and if the IP address range is present in the matching table entry, the packet address is checked as to whether it is within the range; if so, the specified domain is selected; otherwise, the search continues with the next table entry;"
> (Col. 7, lines 61-67)

Appellant respectfully asserts that the Coss reference simply teaches a technique for searching a domain table for an interface name match and the comparison of a packet address to an IP address range. Further, the Minear reference teaches an application layer proxy that includes a plurality of authentication protocols. Nowhere in either of the references, however, is "[a] set of network addresses compris[ing] at least one address outside the zone" mentioned, as claimed by appellant (emphasis added).

In the Advisory Action mailed 04/24/2006, the Examiner argued that Fig. 5A in Coss "indicated the comparison of address versus a table" and that Fig. 7 in Coss "indicates how the address

range is considered and an appropriate response is performed based on the address range." Specifically, Fig. 5 indicates a yes/no branch if the "domain [is] in [the] table" and Fig. 7 indicates a yes/no branch if the "packet address [is] within range." Appellant respectfully asserts that the branches indicated in the referenced figures clear fails to disclose "wherein the zone is defined by a set of network addresses, which comprises at least one address outside the zone," as claimed by appellant (emphasis added).

Also, with respect to the present grouping, the Examiner has relied on the following excerpt from the Coss reference, along with Claim 8 from the Minear reference (reproduced above), to make a prior art showing of appellant's claimed technique "wherein the network address dynamically assigned to the network adapter is determined by at least one of: mapping an adapter registry identifier to an associated network address stored in an operating system registry; monitoring network traffic at the network adapter and examining a predefined limited amount of the network traffic to determine the network address; and receiving a network address from a network adapter device driver when the network adapter connects to the TCP/IP network."

> "...example, specific source and destination port numbers. They can be loaded at any time by trusted parties, e.g., a trusted application, remote proxy or firewall administrator, to authorize specific network sessions. A dynamic rule can be set for..." (Col. 9, lines 6-9)

Appellant respectfully asserts that the Coss reference simply teaches the loading of dynamic rules and that the Minear reference merely teaches an application layer proxy that includes a plurality of authentication protocols. Appellant, on the other hand, claims the determination of the network address dynamically assigned to the network adapter "by [at least one of] mapping an adapter registry identifier to an associated network address stored in an operating system registry; monitoring network traffic at the network adapter and examining a predefined limited amount of the network traffic to determine the network address; and receiving a network address from a network adapter device driver when the network adapter connects to the TCP/IP network," as claimed (emphasis added). The prior art makes no mention of the determination of a network address, much less in the specific context claimed by appellant.

In the Advisory Action mailed 04/24/2006, the Examiner, in a blanket manner, relied upon NETBIOS RFC 1001, MANET RFC 2501, and DHCP RFC 2131 to make a prior art showing of

appellant's claimed technique. Appellant respectfully points out that, specifically, page 10 of the NETBIOS RFC 1001 merely discloses that "NetBIOS resources are referenced by name" and that "an application, representing a resource, registers one or more names that it wishes to use." However, referencing a resource by name simply fails to disclose a technique "wherein the network address dynamically assigned to the network adapter is determined by...mapping an adapter registry identifier to an associated network address stored in an operating system registry," as claimed by appellant (emphasis added).

In addition, pages 4 and 5 of the MANET RFC 2501 simply disclose that '[t]he concept of a "node identifier" (separate and apart from the concept of an "interface identifier") is crucial to supporting the multigraph topology of the routing fabric.' MANET continues to disclose that this node identifier "is what *unifies* a set of wireless interfaces and identifies them as belonging to the same mobile platform [which] permits maximum flexibility in address assignment." However, the node identifiers as disclosed in MANET simply fails to even suggest the technique "wherein the network address dynamically assigned to the network adapter is determined by...monitoring network traffic at the network adapter and examining a predefined limited amount of the network traffic to determine the network address," as claimed by appellant (emphasis added).

Furthermore, pages 12 and 15 of DHCP RFC 2131 simply teach that "[t]he client broadcasts a DHCPDISCOVER message on its local physical subnet" and "[t]he server selected in the DHCPREQUEST message commits the binding for the client to persistent storage and responds with a DHCPACK message containing the configuration parameters for the requesting client." However, this client request and server response fail to disclose a technique "wherein the network address dynamically assigned to the network adapter is determined by...receiving a network address from a network adapter device driver when the network adapter connects to the TCP/IP network," as claimed by appellant (emphasis added).

Moreover, appellant notes that the Examiner fails to cite specific motivation in the above references to support the case for combining the NETBIOS RFC 1001, the MANET RFC 2501 and the DHCP RFC 2131 references. The Examiner is reminded that the Federal Circuit requires that there must be some logical reason apparent from the evidence of record that would justify

the combination or modification of references. *In re Regel, 188 USPQ 132 (CCPA 1975).* Thus, without specific motivation, appellant respectfully asserts that reliance on such references is inappropriate.

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on appellant's disclosure. *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed.Cir.1991).

Appellant respectfully asserts that at least the first and third elements of the *prima facie* case of obviousness have not been met, as noted above

Group #2: Claims 6, 13 and 28

With respect to the current grouping, the Examiner has relied on the following excerpt from the Coss reference to make a prior art showing of appellant's claimed "assigning the security policy to the zone."

> "In the firewall, a decision module or engine, here called a 'domain support engine' (DSE) determines which security policy to use for a new network session. Each new session must be approved by the security policies of the source domain and the destination domain(s). For connections going to the Internet, it is likely that only a single domain check is performed. The DSE makes the domain selection based on the incoming or outgoing network interface, as well as on the source or destination network address of each packet. Inclusion, in packets, of source or destination addresses allows for multiple users to be supported by a single network interface. The incoming or outgoing network interface may be in the form of a network interface card (NIC), e.g., an Intel EtherExpress Pro 100B card available from Intel Corporation." (Col. 6, lines 48-61)

Specifically, the Examiner stated that the above citation "allows for the policies to be applied to zones." However, appellant respectfully disagrees with such argument and points out that the

cited reference merely discloses "determin[ing] which security policy to use for a new network session" and that "[e]ach new session must be approved by the security policies of the source domain and the destination domain(s)." Appellant respectfully asserts that the determination of a security policy for a new network session and the approval of a new session by security policies are quite different from "assigning the security policy to the zone," as claimed by appellant (emphasis added).

Again, appellant respectfully asserts that at least the first and third elements of the *prima facie* case of obviousness have not been met, as noted above.

Group #3: Claims 10, 17 and 30

With respect to the present grouping, the Examiner has relied on Col. 9, lines 6-9 of the Coss reference (shown above) to make a prior art showing of appellant's claimed "receiving data from a predetermined location on the network through the network adapter; and creating the policy file from the data." Specifically, the Examiner argues that this reference citation "allows for the downloading of policies."

Appellant respectfully asserts that the Coss reference merely teaches the loading of dynamic rules "at any time by trusted parties, e.g., a trusted application, remote proxy or firewall administrator, to authorize specific network sessions." Clearly, loading dynamic rules does not even suggest "receiving data from a predetermined location on the network through the network adapter; and creating the policy file from the data," as claimed by the appellant (emphasis added).

Again, appellant respectfully asserts that at least the first and third elements of the *prima facie* case of obviousness have not been met, as noted above.

In view of the remarks set forth hereinabove, all of the independent claims are deemed allowable, along with any claims depending therefrom.

VIII CLAIMS APPENDIX (37 C.F.R. § 41.37(c)(1)(viii))

The text of the claims involved in the appeal (along with associated status information) is set forth below:

1. (Previously Presented) A computerized method for automatically configuring a firewall operating within an individual computer comprising:

determining a zone for a network address dynamically assigned to a network adapter in the individual computer; and

associating a security policy for the zone with the network adapter, the security policy specifying the firewall configuration to protect the individual computer;

wherein the security policy is defined by a policy file which includes a policy file data structure stored as an XML (extensible markup language) document;

wherein a security policy section of the policy file data structure includes an entry for each security policy that is identified by a policy identifier field and is associated with a network protocol that is identified by a protocol identifier field;

wherein the security policy section specifies filters for at least a portion of ports and services defined by the network protocol, and each port and service associated with the security policy is identified by an element identifier field, a field containing filter settings, and a log indicator field;

wherein at least one security policy is included for a TCP/IP network and includes a PPTP (point-to-point tunneling protocol), a RIP (routing information protocol), a DHCP (dynamic host configuration protocol), an ARP (address resolution protocol), an Ident (identification protocol), ICMP (internet control message protocol) and VPN (virtual private networking) ports, and a NetBIOS (network basic input/output system) service;

wherein a default setting for a high security policy on the TCP/IP network disallows incoming network traffic through the PPTP and ICMP ports, allows incoming network traffic through the RIP, DHCP, ARP and VPN ports, disallows access through the NetBIOS service to shared resources on the individual computer, and disallows the individual computer from using shared resources of other computers on the TCP/IP network, where incoming network traffic that attempts to access the individual computer using PPTP and NetBIOS is logged;

wherein a zone section of the policy file data structure includes an entry for each defined address zone and includes an identifier field, an address parameters field that defines the zone, and an identifier field for the security policy assigned to the zone;

wherein a default zone is defined by addresses that are outside another zone;

wherein the determining and associating is performed when the network address for the network adapter changes;

wherein the security policy associated with the network protocol is specific to the network protocol;

wherein the zone is defined by a set of network addresses, which comprises at least one address outside the zone;

wherein the network address dynamically assigned to the network adapter is determined by at least one of:

mapping an adapter registry identifier to an associated network address stored in an operating system registry;

monitoring network traffic at the network adapter and examining a predefined limited amount of the network traffic to determine the network address; and

receiving a network address from a network adapter device driver when the network adapter connects to the TCP/IP network.

2. (Original) The computerized method of claim 1 further comprising:

determining the network address assigned to the network adapter.

3. (Cancelled)

4. (Previously Presented) The computerized method of claim 1, wherein the set of network addresses comprises at least one address within the zone.

5. (Cancelled)

6. (Original) The computerized method of claim 1 further comprising:

assigning the security policy to the zone.

7. (Previously Presented) The computerized method of claim 1 further comprising:

retrieving the policy file that contains definitions for the zone and the security policy and specifies that the security policy is assigned to the zone.

8. (Original) The computerized method of claim 7 further comprising:

creating the policy file from data input by a user.

9. (Original) The computerized method of claim 7 further comprising:

creating the policy file from data input by an administrator.

10. (Previously Presented) The computerized method of claim 7 further comprising:

receiving data from a predetermined location on the network through the network adapter; and

creating the policy file from the data.

11. (Previously Presented) A computer-readable medium having computer-executable instructions to automatically configure a firewall operating within an individual computer comprising:

determining a zone for a network address assigned dynamically to a network adapter in the individual computer;

defining the zone based on a set of network addresses including at least one address outside the zone; and

associating a security policy for the zone with the network adapter, the security policy specifying the firewall configuration to protect the individual computer;

wherein the security policy is defined by a policy file which includes a policy file data structure stored as an XML (extensible markup language) document;

wherein a security policy section of the policy file data structure includes an entry for each security policy that is identified by a policy identifier field and is associated with a network protocol that is identified by a protocol identifier field;

wherein the security policy section specifies filters for at least a portion of ports and services defined by the network protocol, and each port and service associated with the security policy is identified by an element identifier field, a field containing filter settings, and a log indicator field;

wherein at least one security policy is included for a TCP/IP network and includes a PPTP (point-to-point tunneling protocol), a RIP (routing information protocol), a DHCP (dynamic host configuration protocol), an ARP (address resolution protocol), an Ident (identification protocol), ICMP (internet control message protocol) and VPN (virtual private networking) ports, and a NetBIOS (network basic input/output system) service;

wherein a default setting for a high security policy on the TCP/IP network disallows incoming network traffic through the PPTP and ICMP ports, allows incoming network traffic through the RIP, DHCP, ARP and VPN ports, disallows access through the NetBIOS service to shared resources on the individual computer, and disallows the individual computer from using shared resources of other computers on the TCP/IP network, where incoming network traffic that attempts to access the individual computer using PPTP and NetBIOS is logged;

wherein a zone section of the policy file data structure includes an entry for each defined address zone and includes an identifier field, an address parameters field that defines the zone, and an identifier field for the security policy assigned to the zone;

wherein a default zone is defined by addresses that are outside another zone;

wherein the determining and associating is performed when the network address for the network adapter changes;

wherein the security policy associated with the network protocol is specific to the network protocol;

wherein the network address dynamically assigned to the network adapter is determined by at least one of:

mapping an adapter registry identifier to an associated network address stored in an operating system registry;

monitoring network traffic at the network adapter and examining a predefined limited amount of the network traffic to determine the network address; and

receiving a network address from a network adapter device driver when the network adapter connects to the TCP/IP network.

12. (Original) The computer-readable medium of claim 11 having further computer-readable instructions comprising:

determining the network address assigned to the network adapter.

13. (Original) The computer-readable medium of claim 11 having further computer-readable instructions comprising:

assigning the security policy to the zone.

14. (Previously Presented) The computer-readable medium of claim 11 having further computer-readable instructions comprising:

retrieving the policy file that contains definitions for the zone and the security policy and specifies that the security policy is assigned to the zone.

15. (Original) The computer-readable medium of claim 14 having further computer-readable instructions comprising:

creating the policy file from data input by a user.

16. (Original) The computer-readable medium of claim 14 having further computer-readable instructions comprising:

creating the policy file from data input by an administrator.

17. (Previously Presented) The computer-readable medium of claim 14 having further computer-readable instructions comprising:

receiving data from a predetermined location on the network through the network adapter; and

creating the policy file from the data.

18. (Cancelled)

19. (Previously Presented) The computer-readable medium of claim 11 having further computer-readable instructions comprising:

including at least one address within the zone in the set of network addresses.

20. (Cancelled)

21. (Previously Presented) A computerized system comprising:

a processing unit;

a memory coupled to the processing unit through a bus;

a network adapter coupled to the processing unit through the bus and further operable for coupling to a network;

a firewall process executed from the memory by the processing unit to protect the computerized system when the network adapter is coupled to a network by causing the processing unit to filter data addressed to the network adapter according to a security policy; and

a firewall configuration process executed from the memory by the processing unit to cause the processing unit to determine a zone for a network address dynamically assigned to the network adapter and to associate a firewall security policy for the zone with the network adapter;

wherein the security policy is defined by a policy file which includes a policy file data structure stored as an XML (extensible markup language) document;

wherein a security policy section of the policy file data structure includes an entry for each security policy that is identified by a policy identifier field and is associated with a network protocol that is identified by a protocol identifier field;

wherein the security policy section specifies filters for at least a portion of ports and services defined by the network protocol, and each port and service associated with the security policy is identified by an element identifier field, a field containing filter settings, and a log indicator field;

wherein at least one security policy is included for a TCP/IP network and includes a PPTP (point-to-point tunneling protocol), a RIP (routing information protocol), a DHCP (dynamic host configuration protocol), an ARP (address resolution protocol), an Ident (identification protocol), ICMP (internet control message protocol) and VPN (virtual private networking) ports, and a NetBIOS (network basic input/output system) service;

wherein a default setting for a high security policy on the TCP/IP network disallows incoming network traffic through the PPTP and ICMP ports, allows incoming network traffic through the RIP, DHCP, ARP and VPN ports, disallows access through the NetBIOS service to shared resources on the individual computer, and disallows the individual computer from using shared resources of other computers on the TCP/IP network, where incoming network traffic that attempts to access the individual computer using PPTP and NetBIOS is logged;

wherein a zone section of the policy file data structure includes an entry for each defined address zone and includes an identifier field, an address parameters field that defines the zone, and an identifier field for the security policy assigned to the zone;

wherein a default zone is defined by addresses that are outside another zone;

wherein the firewall configuration process is executed by the processing unit when the network address for the network adapter changes;

wherein the security policy associated with the network protocol is specific to the network protocol;

wherein the firewall configuration process further causes the processing unit to define the zone based on a set of network addresses comprising at least one address outside the zone;

wherein the network address dynamically assigned to the network adapter is determined by at least one of:

mapping an adapter registry identifier to an associated network address stored in an operating system registry;

monitoring network traffic at the network adapter and examining a predefined limited amount of the network traffic to determine the network address; and

receiving a network address from a network adapter device driver when the network adapter connects to the TCP/IP network.

22. (Cancelled)

23. (Cancelled)

24. (Original) The computerized system of claim 21 wherein the firewall configuration process further causes the processing unit to determine the network address of the network adapter.

25. (Cancelled)

26. (Previously Presented) The computerized system of claim , wherein the set of network addresses comprises at least one address within the zone.

27. (Cancelled)

28. (Previously Presented) The computerized system of claim 21, wherein the firewall configuration process further causes the processing unit to assign the security policy to the zone.

29. (Previously Presented) The computerized system of claim 21, wherein the firewall configuration process further causes the processing unit to retrieve the policy file that contains definitions for the zone and the security policy and specifies that the security policy is assigned to the zone.

30. (Previously Presented) The computerized system of claim 29, wherein the firewall configuration process further causes the processing unit to receive data from a user and to create the policy file from the data.

31. (Previously Presented) The computerized system of claim 29, wherein the firewall configuration process further causes the processing unit to receive data from an administrator and to create the policy file from the data.

32. (Previously Presented) The computerized system of claim 29, wherein the firewall configuration process further causes the processing unit to receive data from a predetermined location on the network through the network adapter and to create the policy file from the data.

33-43. (Cancelled)

IX EVIDENCE APPENDIX (37 C.F.R. § 41.37(c)(1)(ix))

There is no such evidence.

X RELATED PROCEEDING APPENDIX (37 C.F.R. § 41.37(c)(1)(x))

N/A

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 971-2573. For payment of any additional fees due in connection with the filing of this paper, the Commissioner is authorized to charge such fees to Deposit Account No. 50-1351 (Order No. NAI1P361/00.166.01).

Respectfully submitted,

By: _____ Date: 12/15/06

Kevin J. Zilka

Reg. No. 41,429

Zilka-Kotab, P.C.
P.O. Box 721120
San Jose, California 95172-1120
Telephone: (408) 971-2573
Facsimile: (408) 971-4660